A construction of $\mathbb{F}_2$-linear cyclic, MDS codes

Sara D. Cardell, Joan-Josep Climent, Daniel Panario, Brett Stevens

February 17, 2021

Sara D. Cardell

Instituto de Matemática, Estatística e Computação Científica
Universidade Estadual de Campinas
Campinas, Brazil

Joan-Josep Climent

Departament de Matemàtiques
Universitat d'Alacant
Alacant, Spain

Daniel Panario and Brett Stevens

School of Mathematics and Statistics
Carleton University
Ottawa, Canada

(Communicated by the associate editor name)

Abstract

In this paper we construct $\mathbb{F}_2$-linear codes over $\mathbb{F}_2^b$ with length n and dimension $n - r$ where $n = rb$. These codes have good properties, namely cyclicity, low density parity-check matrices and maximum distance separation in some cases. For the construction, we consider an odd prime p, let $n = p - 1$ and utilize a partition of $\mathbb{Z}_n$. Then we apply a Zech logarithm to the elements of these sets and use the results to construct an *index array* which represents the parity-check matrix of the code. These codes are always cyclic and the density of the parity-check and the generator matrices decreases to 0 as n grows (for a fixed r). When $r = 2$ we can prove that these codes are always maximum distance separable. For higher r some of them retain this property.

*The first author was supported by CAPES (Brazil). The work of the second author was partially supported by Spanish grants AICO/2017/128 of the Generalitat Valenciana and VIGROB287 of the Universitat d'Alacant. The third and fourth authors were supported by NSERC (Canada).

1 Introduction

The class of $\mathbb{F}_q$-linear codes have been widely studied [1, 3, 6, 17, 18]. They have various applications in communication and storage systems, where the alphabet size is typically large, to protect data against erasures [1, 3]. They can be also employed to organize redundant data into disk arrays [2, 10].

These codes are very useful to dynamic high-speed storage applications since they have low-complexity decoding algorithms over small fields and low update complexity when small changes are applied to the stored data [4]. In general, Reed-Solomon codes have none of these properties; thus, $\mathbb{F}_q$-linear codes are more efficient than Reed-Solomon codes in computational complexity terms [4]. In this article we construct $\mathbb{F}_2$-linear codes which are cyclic, have low density parity check and generator matrices and in some cases are MDS (maximum distance separable) [14]. MDS codes provide the maximum protection against device failure for a given amount of redundancy [3]. Cyclic codes provide great advantages such as concise representations and efficient encoding and decoding. Furthermore, if the parity-check matrix of the code is low density, in particular if we have an upper bound on the number of non-zero entries in each column, then the matrix can provide information about where an error might have occurred [15].

It is possible to find some constructions of these kinds of codes in [1, 5, 8, 13, 16, 17].

In Section 2 we introduce some notation and concepts that we need to follow the paper. In Section 3 we present the construction of an index array that represents a parity-check matrix of $\mathbb{F}_q$-linear code and in Section 4 we mention the properties of this construction. Finally, we also introduce a decoding algorithm in Section 5.

2 Preliminaries

We start this section with the definition of $\mathbb{F}_q$-linear codes [6, 13].

Definition 2.1: Let b be a positive integer. A code $\mathcal{C}_{\mathbb{F}_q^b}$ is said to be an **$\mathbb{F}_q$-linear code** of length n over $\mathbb{F}_q^b$ if it is a linear subspace of the vector space $\mathbb{F}_q^{nb}$. Equivalently it is an $\mathbb{F}_q$-linear code over $\mathbb{F}_q^b$ if the code $\mathcal{C}_{\mathbb{F}_q}$ is a linear code of length nb over $\mathbb{F}_q$.

Notice that both $\mathcal{C}_{\mathbb{F}_q}$ and $\mathcal{C}_{\mathbb{F}_q^b}$ refer to the same set of codewords, but over the alphabets $\mathbb{F}_q$ and $\mathbb{F}_q^b$, respectively. Therefore, the codewords of $\mathcal{C}_{\mathbb{F}_q^b}$ of length n over $\mathbb{F}_q^b$ can also be viewed as codewords of length nb over $\mathbb{F}_q$. It is worth pointing out that the code symbols of $\mathcal{C}_{\mathbb{F}_q^b}$ can be regarded as elements in the field $\mathbb{F}_{q^b}$. However, linearity over this field is not assumed.

Now, we analyze the relationship between the parameters of the code over $\mathbb{F}_q$ and the parameters of the code over $\mathbb{F}_q^b$. Let $[N, K, D]$ denote the parameters of the code $\mathcal{C}_{\mathbb{F}_q}$ over $\mathbb{F}_q$. The number $k = \log_{q^b}\left|\mathcal{C}_{\mathbb{F}_q^b}\right|$ is the **normalized dimension** (or just dimension) of $\mathcal{C}_{\mathbb{F}_q^b}$ over $\mathbb{F}_q^b$. If b divides K then $k = K/b$ (in what follows, b divides K). Thus, the parameters of the code $\mathcal{C}_{\mathbb{F}_q^b}$ are $[n, k, d]$ over $\mathbb{F}_q^b$, where d is the minimum distance and $n = N/b$. To define the minimum (Hamming) distance of $\mathcal{C}_{\mathbb{F}_q^b}$ we consider it as a code over the alphabet $\mathbb{F}_q^b$. Then, the distance d is measured with respect to the symbols of $\mathbb{F}_q^b$ (see [6]).

It is worth remembering that the code $\mathcal{C}_{\mathbb{F}_q^b}$ can be specified by either its parity-check matrix H of size $(n-k)b \times nb$ or its generator matrix G of size $kb \times nb$, both over $\mathbb{F}_q$. The matrix H (respectively, G) is said to be **systematic** if it contains the identity matrix of size $(n-k)b \times (n-k)b$ (respectively, $kb \times kb$).

Example 1: Consider the generator matrix G given by

$$G = \left[\begin{array}{cccc:cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right].$$

This matrix is in systematic form and is a generator matrix of a code $\mathcal{C}_{\mathbb{F}_2}$ of length 8 and dimension 4 over $\mathbb{F}_2$.

We can compute the sixteen codewords of the code, and we can divide the bits of each codeword into groups of two elements. Then if we consider the codewords over the new alphabet $\mathbb{F}_2^2$, the length of each codeword is 4 and the normalized dimension of our new code $\mathcal{C}_{\mathbb{F}_2^2}$ is $4/2 = 2$. Then, the generator matrix can be seen as the block matrix

$$G = \left[\begin{array}{c:c:c:c} 1 \; 0 & 0 \; 0 & 1 \; 1 & 1 \; 1 \\ 0 \; 1 & 0 \; 0 & 1 \; 0 & 1 \; 0 \\ 0 \; 0 & 1 \; 0 & 1 \; 1 & 0 \; 1 \\ 0 \; 0 & 0 \; 1 & 0 \; 1 & 1 \; 0 \end{array}\right].$$

Then the length of the code $\mathcal{C}_{\mathbb{F}_q}$ is 8, the dimension is 4 and the minimum distance is 3. It is possible to check that the minimum distance of the code $\mathcal{C}_{\mathbb{F}_2^2}$ is also 3.

In general, the minimum distance of $\mathcal{C}_{\mathbb{F}_q}$ over $\mathbb{F}_q$ is greater than or equal to the minimum distance of $\mathcal{C}_{\mathbb{F}_q^b}$ over $\mathbb{F}_q^b$ [7]. It is worth pointing out that though this distance is greater it does not mean that the code is better. We cannot compare these two codes, since both alphabets are different.

Now, we are ready to introduce the concept of MDS $\mathbb{F}_q$-linear code.

Definition 2.2: An $\mathbb{F}_q$-linear code with parameters $[n, k, d]$ is **MDS** (maximum distance separable) over $\mathbb{F}_q^b$ if the Singleton bound

$$d \leq n - k + 1$$

is attained [6].

The correcting capacity of a code depends on the minimum distance and the higher the minimum distance is, the more errors the code can correct.

In Example 1, it is possible to check that the distances between all pairs of codewords of the code $\mathcal{C}_{\mathbb{F}_2^2}$ only take the values 3 or 4 over $\mathbb{F}_2^2$. Thus the minimum distance of the code is 3. Since the length is 4 and the dimension is 2, the code is an MDS $\mathbb{F}_2$-linear code over $\mathbb{F}_2^2$.

The following theorems provide very useful characterizations in order to check whether an $\mathbb{F}_q$-linear code is MDS or not without computing the minimum distance. These theorems are an extension of the characterization theorems for MDS block codes given in [14]. The first theorem can be used when we have the parity-check matrix of the code. The second one allows us to check if the code is MDS when we have either the generator or the parity-check matrix in systematic form.

Theorem 2.3: *[6, Proposition 3.1] Let $H = [H_0 \; H_1 \; \ldots \; H_{n-1}]$ be an $(n-k)b \times nb$ parity-check matrix of an $\mathbb{F}_q$-linear code $\mathcal{C}_{\mathbb{F}_q^b}$ with parameters $[n, k]$ over $\mathbb{F}_q^b$, where each H_i is an $(n-k)b \times b$ submatrix of H. Then $\mathcal{C}_{\mathbb{F}_q^b}$ is MDS if and only if the $(n-k)b$ columns of any $n-k$ distinct submatrices H_i form a linearly independent set over $\mathbb{F}_q$.*

Theorem 2.4: *[6, Proposition 3.2] Let $H = \left[A \; I_{(n-k)b}\right]$ be an $(n-k)b \times nb$ systematic parity-check matrix of an $\mathbb{F}_q$-linear code $\mathcal{C}_{\mathbb{F}_q^b}$ with parameters $[n, k]$ over $\mathbb{F}_q^b$ and write $A = [A_{i,j}] \in \mathrm{Mat}_{(n-k)b \times kb}(\mathbb{F}_q^b)$, where each $A_{i,j}$ is a $b \times b$ block submatrix of A. Then $\mathcal{C}_{\mathbb{F}_q^b}$ is MDS if and only if every square submatrix of A consisting of full blocks submatrices $A_{i,j}$ is non-singular.*

We will use Theorem 2.4 to show that our codes for $r = 2$ are MDS in Section 4.2.

The next example illustrates the idea given in the previous theorems.

Example 2: We consider the code $\mathcal{C}_{\mathbb{F}_2^2}$ with parameters $[4, 2]$ over $\mathbb{F}_2^2$, whose parity-check matrix is

$$H = [A \;\; I_4] = \left[\begin{array}{cc:cc:cc:cc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hdashline 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hdashline 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ \hdashline 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

Since the matrices

$$A_{1,1} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad A_{1,2} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad A_{2,1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad A_{2,2} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and A are non-singular, according to Theorem 2.4, the code is MDS over $\mathbb{F}_2^2$.

Next, we introduce an important theorem that implies that the $\mathbb{F}_q$-dual of an $\mathbb{F}_q$-linear code is MDS if and only if the original code is MDS.

Theorem 2.5: *Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear code over $\mathbb{F}_q^b$ and $\mathcal{C}^\perp$ be the dual code over $\mathbb{F}_q$ which is also an $\mathbb{F}_q$-linear code over $\mathbb{F}_q^b$. Then $\mathcal{C}$ is MDS if and only if $C^\perp$ is MDS.*

Proof: Suppose the parameters of $\mathcal{C}$ over $\mathbb{F}_q^b$ are $[n, k, d]$ and let $H = [H_0 \; H_1 \; \ldots \; H_{n-1}]$ be its $(n-k)b \times nb$ parity-check matrix over $\mathbb{F}_q$. The parameters of $\mathcal{C}^\perp$ are $[n, n-k, \delta]$ and H is a generator matrix for $\mathcal{C}^\perp$ over $\mathbb{F}_q$. If $\mathcal{C}$ is MDS then $d = n - k + 1$. Suppose that $\boldsymbol{c}$ is a word in $C^\perp$ of minimum non-zero $\mathbb{F}_q^b$-weight δ. The Singleton bound implies that $\delta \leq n - (n-k) + 1 = k + 1$. We need to show that $\delta \geq k + 1$. Suppose that $\delta \leq k$. Thus the support of $\boldsymbol{c}$ is contained in the positions corresponding to the columns of no more than k of the submatrices H_i. Let $\mathcal{H}$ be a set of k submatrices H_i which contain the support of $\boldsymbol{c}$. The codeword $\boldsymbol{c}$ is a non-trivial linear combination of the rows of H. By Theorem 2.3 the $b(n-k) \times b(n-k)$ matrix formed from the submatrices $H_i \notin \mathcal{H}$ is rank $b(n-k)$. Restricting attention to just these positions in code $\mathcal{C}^\perp$, c is the zero vector and is a non trivial linear combination of the rows of a full rank square matrix which is a contradiction.

Now, we define the concept of cyclicity for $\mathbb{F}_q$-linear codes.

Definition 2.6: An $\mathbb{F}_q$-linear code $\mathcal{C}_{\mathbb{F}_q^b}$ with length n over $\mathbb{F}_q^b$ is **cyclic** if $[\boldsymbol{c}_0 \; \boldsymbol{c}_1 \; \ldots \; \boldsymbol{c}_{n-1}] \in \mathcal{C}_{\mathbb{F}_q^b}$ implies that $[\boldsymbol{c}_{n-1} \; \boldsymbol{c}_0 \; \boldsymbol{c}_1 \; \ldots \; \boldsymbol{c}_{n-2}] \in \mathcal{C}_{\mathbb{F}_q^b}$.

It is worth pointing out that $\boldsymbol{c}_i \in \mathbb{F}_q^b$, for $i = 0, 1, \ldots, n-1$. Therefore, the code $\mathcal{C}_{\mathbb{F}_q^b}$ is cyclic if and only if $\mathcal{C}_{\mathbb{F}_q}$ is quasi-cyclic of index b.

Consider P the matrix which shifts the columns of the matrix H b positions to the right. That is, if $H = [H_0 \; H_1 \; \ldots \; H_{n-1}]$, with H_i a block of size $(n-k)b \times b$, then $H \cdot P = [H_{n-1} \; H_0 \; H_1 \; \ldots \; H_{n-2}]$.

More specifically P is the $nb \times nb$ matrix given by

$$P = \begin{bmatrix} 0 & I_b & 0 & \cdots & 0 \\ 0 & 0 & I_b & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & I_b \\ I_b & 0 & 0 & \cdots & 0 \end{bmatrix} \tag{1}$$

where 0 denotes the $b \times b$ zero matrix. The cyclicity of the code is related to the following property, whose proof is straightforward.

Theorem 2.7: *An $\mathbb{F}_q$-linear code $\mathcal{C}_{\mathbb{F}_q^b}$ over $\mathbb{F}_q^b$ with parity-check matrix H is cyclic if and only if there exists an invertible matrix L_P of size $(n-k)b \times (n-k)b$ such that $H \cdot P = L_P \cdot H$.*

The next example helps us to understand this idea.

Example 3: Consider the parity-check matrix of a code $\mathcal{C}_{\mathbb{F}_2^2}$ given by

$$H = \left[\begin{array}{cc:cc:cc:cc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right].$$

If we shift each block column one position to the right, wrapping the last block column around to the first position, we obtain the following matrix

$$H \cdot P = \left[\begin{array}{cc:cc:cc:cc} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right] = L_P \cdot H$$

where P is defined by (1) and L_P has the form:

$$L_P = \left[\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{array}\right].$$

As we can see, the rows are the same, but shifted one position up and the first row becomes the last one. As a consequence we can confirm that the code is cyclic. ■

3 Construction

We introduce the concept of index array, a table that stores the positions of the non-zero elements in a binary matrix.

Definition 3.1: Let $\mathcal{C}_{\mathbb{F}_2^b}$ be an $\mathbb{F}_2$-linear code with parameters $[n, k]$ over $\mathbb{F}_2^b$ and let $H = [h_{i,j}]$ be an $(n-k)b \times nb$ parity-check matrix of $\mathcal{C}_{\mathbb{F}_2^b}$ over $\mathbb{F}_2$. The matrix H can be represented by a $b \times n$ array of sets. The cell in location (i, j) contains the set $\{t \mid h_{t,i+bj} = 1\}$. This array is called **index array** of H.

Basically, each cell of an index array represents a column of the parity-check matrix, and inside the cell we store the position of the 1s in the corresponding column. We often refer to an index array just with array.

Given a matrix of size $m \times n$ the numeration of rows (respectively, columns) starts with 0 and ends with $m - 1$ (respectively, $n - 1$). The following example clarifies this definition.

Example 4: We consider the linear code $\mathcal{C}_{\mathbb{F}_2}$ with parameters $[18, 12]$ over $\mathbb{F}_2$, whose parity-check matrix is given by

$$H = \left[\begin{array}{ccc:ccc:ccc:ccc:ccc:ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right].$$

Of course, this code can be also seen as an $\mathbb{F}_2$-linear code $\mathcal{C}_{\mathbb{F}_2^3}$ with parameters $[6, 4]$ over $\mathbb{F}_2^3$. We can represent the matrix H by the index array

$$A_H = \begin{array}{|c|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 4,5 & 5,0 & 0,1 & 1,2 & 2,3 & 3,4 \\ \hline 1,3 & 2,4 & 3,5 & 4,0 & 5,1 & 0,2 \\ \hline \end{array}$$

where each cell represents each column of H and each block column of the array represents each block of columns of H. ■

Now, we need to recall the concept of Zech logarithm [9, 11].

Definition 3.2: Let α be a primitive element of $\mathbb{F}_p$, with p a prime integer. The **Zech logarithm** with base α is the bijective map

$$\mathcal{Z}_\alpha : \mathbb{Z}_{p-1} \cup \{\infty\} \longrightarrow \mathbb{Z}_{p-1} \cup \{\infty\}$$

where $\alpha^\infty = 0$ by convention and $\alpha^x + 1 = \alpha^{\mathcal{Z}_\alpha(x)}$.

Now, we are ready to construct an index array which represents a parity-check matrix of an $\mathbb{F}_2$-linear code over $\mathbb{F}_2^b$. We will explore these codes properties in Section 4.

Let p be an odd prime integer, α be a primitive element of $\mathbb{F}_p$ and let $n = p - 1 = rb$. Define $u = n/2 \bmod b$. We construct an index array corresponding to the parity-check matrix H of an $\mathbb{F}_2$-linear code with parameters $[n, k]$ over $\mathbb{F}_2^b$, where $k = n - r$.

Let

$$E_i = \{x \in \mathbb{Z}_n \mid i = x \bmod b\}, \quad i = 0, 1, \ldots, b-1, \tag{2}$$

which form a partition of $\mathbb{Z}_n$ and for $i \neq u$ let $D_i = \mathcal{Z}_\alpha(E_i)$. Each set E_i (and D_i) contains r elements. We eliminate E_u because $n/2 \in E_{n/2}$ and $\mathcal{Z}_\alpha(n/2) = \infty \notin \mathbb{Z}_n$. To deal with the indexing caused by this elimination, let $\lambda(i, u)$ be the indicator function of $i \leq u$ and $\gamma(i, u)$ be the indicator function of $i \geq u$. Finally let $A(p, r, \alpha)$ be the $b \times n$ index array given by

$$A(p, r, \alpha)_{ij} = \begin{cases} \{j\}, & i = 0, \\ D_{i-\lambda(i,u)} + j, & i > 0. \end{cases} \tag{3}$$

This index array corresponds to the $rb \times nb$ parity check matrix $H(p, r, \alpha)$ defined by

$$H(p, r, \alpha)_{ij} = \begin{cases} 1, & ib = j, \\ 1, & i \in D_{z-\lambda(z,u)},\ j = \ell b + z,\ 1 \leq z < b,\ 0 \leq \ell < n, \\ 0, & \text{otherwise.} \end{cases}$$

We define $C(p, r, \alpha)$ to be the $\mathbb{F}_2$-linear code over $\mathbb{F}_2^b$ with $H(p, r, \alpha)$ as its parity check matrix over $\mathbb{F}_2$. The index array $A(p, r, \alpha)$ is shown in Table 1.

Let $G(p, r, \alpha)$ be the $n(b-1) \times nb$ matrix over $\mathbb{F}_2$ defined by

$$G(p, r, \alpha)_{ij} = \begin{cases} 1, & j = i + \ell + 1,\ i = \ell(b-1) + z,\ 1 \leq z < b-1,\ 0 \leq \ell < n, \\ 1, & j \bmod b = 0,\ i = \ell(b-1) + z,\ 0 \leq z < b-1,\ 0 \leq \ell < n, \\ & \quad \text{and } (j/b) \in D_{z+\gamma(z,u)} + \ell, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

Theorem 3.3: *$G(p, r, \alpha)$ is a generator matrix for $C(p, r, \alpha)$ over $\mathbb{F}_2$.*

Proof: We use the fact that $H(p, r, \alpha)$ does contain an $rb \times rb$ identity matrix so it is systematic. Let permutation π be defined by

$$\pi(i) = \begin{cases} n(b-1) + \ell, & \text{if } i = \ell b, \\ \ell(b-1) + z - 1, & \text{if } i = \ell b + z,\ 1 \leq z < b,\ 0 \leq \ell < n. \end{cases}$$

0	1	2	$\cdots$	$p-3$	$p-2$
D_0	D_0+1	D_0+2	$\cdots$	D_0+p-3	D_0+p-2
D_1	D_1+1	D_1+2	$\cdots$	D_1+p-3	D_1+p-2
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
D_{u-1}	$D_{u-1}+1$	$D_{u-1}+2$	$\cdots$	$D_{u-1}+p-3$	$D_{u-1}+p-2$
D_{u+1}	$D_{u+1}+1$	$D_{u+1}+2$	$\cdots$	$D_{u+1}+p-3$	$D_{u+1}+p-2$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
D_{b-1}	$D_{b-1}+1$	$D_{b-1}+2$	$\cdots$	$D_{b-1}+p-3$	$D_{b-1}+p-2$

Table 1: Index array constructed in Section 3.

0	1	2	$\cdots$	$p-3$	$p-2$
D_1	D_1+1	D_1+2	$\cdots$	D_1+p-3	D_1+p-2
D_2	D_2+1	D_2+2	$\cdots$	D_2+p-3	D_2+p-2
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
D_{b-1}	$D_{b-1}+1$	$D_{b-1}+2$	$\cdots$	$D_{b-1}+p-3$	$D_{b-1}+p-2$

Table 2: Index array representing the parity-check matrix when $r=2$.

Applying π to the columns we get H in the form $[H' \;\; I]$. Thus the generator matrix is

$$\begin{bmatrix} I & -H^T \end{bmatrix} = \begin{bmatrix} I & H^T \end{bmatrix}$$

because H is a matrix over $\mathbb{F}_2$ [14]. Applying π^{-1} to the columns of the above matrix gives the matrix $G(p,r,\alpha)$.

The index array of the generator matrix is much simpler to describe. It has the form given in Table 3, where

$$B = \{j : j = \ell(b-1)+z,\ 0 \le z < b-1,\ 0 \le \ell < n,\ 0 \in D_{z+\gamma(z,u)} + \ell\}.$$

Formally, the index array of the generator matrix $G(p,r,\alpha)$, is the $b \times n$ array $B(p,r,\alpha)$ given by

$$B(p,r,\alpha)_{ij} = \begin{cases} B + j(b-1), & i = 0, \\ \{j(b-1)+i-1\}, & i > 0. \end{cases} \tag{5}$$

When $r=2$, then $u=0$ and thus the forms of the generator matrix and its index array are simpler. The index array from Table 1 simplifies to that given in Table 2 and in the computation of B_i, $\gamma(z,0)$ is always 1.

Example 5: Let $p=7$, $n=6$, $r=2$, $b=3$ and $\alpha=3$. The Zech logarithm table is:

x	0	1	2	3	4	5	∞
$\mathcal{Z}_\alpha(x)$	2	4	1	∞	5	3	0

¿From Expression (2) the sets E_i which partition $\mathbb{Z}_6$ are

$$E_0 = \{0,3\}, \quad E_1 = \{1,4\} \quad \text{and} \quad E_2 = \{2,5\}.$$

B	$B+(b-1)$	$B+2(b-1)$	$B+3(b-1)$	$B+4(b-1)$	$\cdots$	$B+(n-1)(b-1)$
0	$b-1$	$2(b-1)$	$3(b-1)$	$4(b-1)$	$\cdots$	$(n-1)(b-1)$
1	b	$2(b-1)+1$	$3(b-1)+1$	$4(b-1)+1$	$\cdots$	$(n-1)(b-1)+1$
2	$b+1$	$2(b-1)+2$	$3(b-1)+2$	$4(b-1)+2$	$\cdots$	$(n-1)(b-1)+2$
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$		$\vdots$
$b-2$	$2b-3$	$3(b-1)-1$	$4(b-1)-1$	$5(b-1)-1$	$\ldots$	$n(b-1)-1$

Table 3: Index array representing the generator matrix computed from the index array in Table 2.

In this case $u = n/2 \bmod b = 0$, so we eliminate the set $E_0 = \{0, 3\}$. Applying the Zech logarithm to the remaining sets we obtain

$$D_1 = \{4, 5\} \quad \text{and} \quad D_2 = \{1, 3\}.$$

Together with $\{0\}$, these sets form the 0th column of the index array, $A(7, 2, 3)$. The rest of the columns of the index array can be obtained from Equation (3) and from the general form shown in Table 1; $A(7, 2, 3)$ and $H(7, 2, 3)$ are given in Example 4, denoted as A_H and H, respectively.

The corresponding generator matrix is

$$G(7,2,3) = \left[\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc} 0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0\\ 0&0&1&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\ 1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0\\ 0&0&0&0&0&1&1&0&0&0&0&0&1&0&0&0&0&0\\ 1&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&1&0&0\\ 0&0&0&1&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0\\ 0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\ 0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&0\\ 1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1 \end{array}\right].$$

The index array representing the generator matrix is given by:

B	$B+2$	$B+4$	$B+6$	$B+8$	$B+10$
0	2	4	6	8	10
1	3	5	7	9	11

$=$

$2,4,7,11$	$1,4,6,9$	$3,6,8,11$	$1,5,8,10$	$0,3,7,10$	$0,2,5,9$
0	2	4	6	8	10
1	3	5	7	9	11

.

■

4 Construction Properties

In this section we show that the codes $C(p, r, \alpha)$ and their duals have desirable properties: cyclicity, MDS and low density matrices.

4.1 Cyclicity

In this section, we prove that the codes we obtained in Section 3 are always cyclic.

Corollary 4.1: *For p a prime, r dividing $n = p - 1$ and α primitive in $\mathbb{F}_p$ the code $C(p, r, \alpha)$ is cyclic.*

Proof: If we observe the form of the array given in Table 1 and we subtract 1 to the elements in the sets, the last column is now the first column as we can see in Table 4.

Let P the matrix defined in (1) and

$$L_P = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

If we denote by H the parity-check matrix represented by the array in Table 1, we have that $H \cdot P = L_P \cdot H$ and this matrix is represented by the array in Table 4. Then, Theorem 2.7 shows that the code is cyclic.

We note that L_P is always the $b \times b$ identity matrix with its columns shifted right once.

Example 6: Consider the index array in Example 4. This array represents the parity-check matrix of an $\mathbb{F}_2$-linear code over $\mathbb{F}_2^3$ with parameters $n = 6$ and $k = 4$ (with $b = 3$ and $r = 2$). Therefore, if we subtract 1 modulo n to every element in every set of the array A_H of Example 4 we obtain the following array

5	0	1	2	3	4
3, 4	4, 5	5, 0	0, 1	1, 2	2, 3
0, 2	1, 3	2, 4	3, 5	4, 0	5, 1

which represents the matrix

$$\left[\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

This matrix is obtained shifting the blocks one position to the right and moving the last block to the beginning. At the same time, this matrix can be also obtain by $H \cdot P = L_p \cdot H$. By Corollary 4.1, the code is cyclic. ■

4.2 Maximum Distance Separability

When $r = 2$ we can show that the codes $C(p, r, \alpha)$ are MDS. We use Theorem 2.3 but first we need some intermediate results.

Let p be an odd prime, $n = p - 1$, $b = n/2$ and α be primitive in $\mathbb{F}_q$. Let $\text{Diffs}_p = \{z \in \mathbb{Z}_p : 1 \leq z \leq b\}$. For each $i \in \mathbb{Z}_p$ let $F_i = \{e_{ij} = \{i + j, i - j\} : j \in \text{Diffs}_p\}$. We observe that F_i is a partition of $\mathbb{Z}_p \setminus \{i\}$. Letting $\log_\alpha : \mathbb{Z}_p \to \mathbb{Z}_n \cup \{\infty\}$ be the discrete logarithm with base α we see that

$$\log_\alpha(F_0) = \{E_i : 0 \leq i < b\},$$

$p-2$	0	1	2	$\cdots$	$p-3$
D_0+p-2	D_0	D_0+1	D_0+2	$\cdots$	D_0+p-3
D_1+p-2	D_1	D_1+1	D_1+2	$\cdots$	D_1+p-3
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
$D_{u-1}+p-2$	D_{u-1}	$D_{u-1}+1$	$D_{u-1}+2$	$\cdots$	$D_{u-1}+p-3$
$D_{u+1}+p-2$	D_{u+1}	$D_{u+1}+1$	$D_{u+1}+2$	$\cdots$	$D_{u+1}+p-3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
$D_{b-1}+p-2$	D_{b-1}	$D_{b-1}+1$	$D_{b-1}+2$	$\cdots$	$D_{b-1}+p-3$

Table 4: Index array obtained by subtracting 1 modulo n to every set in the array given in Table 1.

where E_i are the sets introduced in Equation (2). Similarly for $j \in \mathbb{Z}_n$, and for the sets $D_i = \mathcal{Z}_\alpha(E_i)$, we have that

$$\begin{aligned}
\{D_i + j : 0 \le i < b\} &= \{\ \{\mathcal{Z}_\alpha(i)+j, \mathcal{Z}_\alpha(i+b)+j\} : 0 \le i < b\ \} \\
&= \{\ \{j+\log_\alpha(1+\alpha^i), j+\log_\alpha(1+\alpha^{i+b})\} : 0 \le i < b\ \} \\
&= \{\ \{\log_\alpha(\alpha^j+\alpha^{i+j}), \log_\alpha(\alpha^j+\alpha^{i+j+b})\} : 0 \le i < b\ \} \\
&= \{\ \{\log_\alpha(\alpha^j+\alpha^{i+j}), \log_\alpha(\alpha^j-\alpha^{i+j})\} : 0 \le i < b\ \} \\
&= \log_\alpha(F_{\alpha^j}).
\end{aligned}$$

Finally when $r=2$, $u=0$ so $E_0 = \{0,b\} = \log_\alpha e_{01}$ is discarded. In the place of where D_0+j would go in $A(p,2,\alpha)$ is simply the set $\{j\} = \log(e_{01} \setminus \{0\}) + j$ so it corresponds to what D_0+j would be with the element ∞ removed. Thus the columns of $H(p,2,\alpha)$ that correspond to the jth column of the index array $A(p,2,\alpha)$ are simply the incidence vectors of $\log(F_{\alpha^j})$ ignoring $\log(0)=\infty$. Our goal is to show that the union of the $n=2b$ columns in $H(p,2,\alpha)$ corresponding to any two columns of $A(p,2\alpha)$ are rank n. We will work in the domain of $\log_\alpha$ which is $\mathbb{Z}_p$ rather than in the range, $\mathbb{Z}_n \cup \{\infty\}$. We only need to remember to delete the element $0 \in \mathbb{Z}_p$.

Our first lemma determines the result of addition and multiplication on the elements of F_i.

Lemma 4.2: *For $j \in \mathbb{Z}_p$, $F_i + j = F_{i+j}$. For $z \in \mathbb{Z}_p \setminus \{0\}$, $zF_i = F_{zi}$.*

For the next lemma we think of the F_i as edge sets of a graph whose vertices are the elements of $\mathbb{Z}_p$. With this viewpoint is is easy to check that $F_0 \cup F_1$ is a Hamilton path between vertices $0, 1 \in \mathbb{Z}_p$, that is, a path in the graph that visits each vertex exactly once. The next lemma shows that the union of any two F_i is also a Hamilton path. To express this fact we use the symbol $\cong$ to mean *isomorphic* under either addition by an element of $\mathbb{Z}_p$ or multiplication by an element in $\mathbb{Z}_p \setminus \{0\}$.

Lemma 4.3: *$F_i \cup F_j \cong F_0 \cup F_1$ for any $i \neq j$.*

Proof: By the additive transformation from Lemma 4.2 we have that

$$F_i \cup F_j \cong F_0 \cup F_{j-i}$$

and $j - i \neq 0$. Let $b(j-i) = 1$ in $\mathbb{Z}_p$. Then by the multiplicative transformation from Lemma 4.2

$$F_0 \cup F_{j-i} \cong F_{b0} \cup F_{b(j-i)} = F_0 \cup F_1.$$

Thus $F_i \cup F_j$ is a Hamilton path with i and j as the end vertices. Given any path in a graph, the matrix whose columns are the incidence vectors of the edges of the path together with the incidence vector of one of the end-points of the path has full rank.

Lemma 4.4: *The square matrix, $M_\ell = [m_{ij}] \in \mathrm{Mat}_{\ell\times\ell}(\mathbb{Z}_2)$ defined by*

$$m_{ij} = \begin{cases} 1, & i \le j \le i+1, \\ 0, & \textit{otherwise}, \end{cases}$$

has rank n.

Proof: Adding each column, in order along the path, to the subsequent column in the path, transforms the matrix into the identity. Each of these is an elementary column operation so the rank has not changed.

Theorem 4.5: *Let p be an odd prime and α be primitive in $\mathbb{Z}_p$. The $\mathbb{F}_2$-linear code $C(p, 2, \alpha)$ and its dual code are both MDS.*

Proof: Consider the n columns of H that correspond to columns j_1 and j_2 of $A(p, 2, \alpha)$. By Lemma 4.3, before deleting the point 0 (corresponding to ∞ in the range of log) these columns were the incidence vectors of the edges of a Hamilton path from α^{j_1} to α^{j_2}. After deleting the point 0, the columns are now the incidence vectors of the edges of two vertex-disjoint paths, together with the incidence vectors of one endpoint from each component. Thus after a suitable permutation of rows and columns, this $n \times n$ matrix consists of two blocks (not necessarily of the same size) on the diagonal, each isomorphic to M_ℓ for some ℓ. Thus by Lemma 4.4, this matrix has rank n.

By Theorem 2.5, the dual code is also MDS.

This proof corresponds very closely to the proof that a perfect 1-factorization exists in K_{p+1} for any prime p [12]. We are currently investigating the connections between perfect 1-factorizations and MDS $\mathbb{F}_2$-linear codes.

The codes constructed in Section 3 are not MDS for every value of $r|n$. In Table 5 we report the MDS property for $C(p, r, \alpha)$ for $p \le 43$ and $r \le 15$. For every prime p and value of r, the choice of the primitive element α, did not affect the property of being MDS. That is the code was either MDS for every α or not MDS for every α. Thus we do not include α in our results. The symbol ✔ indicates the code is MDS (and thus its dual also) and symbol ✘ indicates neither code is MDS. In addition to the case $r = 2$, the codes may be MDS when $r = 3$ and $p > 7$. Proving this is our primary future goal.

4.3 Low Density Matrices

The construction here presented yields $\mathbb{F}_2$-linear codes over $\mathbb{F}_2^b$ with parameters $[n, n-r]$, with $b = \frac{n}{r}$. We now show that these codes have the low density parity check matrix property.

Theorem 4.6: *Let p be prime, r divide $n = p - 1$ and α be primitive in $\mathbb{Z}_p$. The number of non-zero elements in the parity check matrix $H(p, r, \alpha)$ is*

$$\frac{n(n-r+1)}{nrb^2} = \frac{nr(n-r+1)}{n^3}.$$

Proof: The number of 1s in each row of the parity-check matrix is $n - r + 1$ (every integer in $\mathbb{Z}_n$, representing each row, appears $n - r + 1$ times in the index array). On the other hand, there are n columns containing one 1 and the number of 1s contained in the remaining $n(b-1)$ columns is r. Therefore, the average number of 1s in the parity-check matrix is

$$\frac{n(n-r+1)}{nrb^2} = \frac{nr(n-r+1)}{n^3}.$$

		p											
		5	7	11	13	17	19	23	29	31	37	41	43
r	2	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	3		×		✔		✔			✔	✔		✔
	4				×	×			✔		✔	×	
	5			×						×		×	
	6				×		×			×	×		×
	7								×				×
	8					×						×	
	9						×				×		
	10									×		×	
	11							×					
	12										×		
	13												
	14								×				×
	15									×			

Table 5: MDS property of $C(p, r, \alpha)$ for different values of p and r.

This leads to the following result.

Corollary 4.7: *Let r be fixed, $p \equiv 1 \pmod{r}$ be prime and α be primitive in $\mathbb{F}_p$. The limit of the number of non-zero elements in $H(p, r, \alpha)$ as $p \to \infty$ is 0.*

Thus the codes $C(p, r, \alpha)$ are LDPC.

In particular, when $r = 2$, that is when the code is proven to be MDS, the average number of ones in the parity-check matrix is

$$\frac{2(n-1)}{n^2}.$$

The generator matrices defined in Equation (4) are also low density.

Theorem 4.8: *Let p be prime, r divide $n = p - 1$ and α be primitive in $\mathbb{Z}_p$. The number of non-zero elements in the generator matrix $G(p, r, \alpha)$ is*

$$\frac{(n-1)r(r+1)}{(n-r)n^2}.$$

Proof: For a fixed value of r, the generator matrix will have $(n - r)b$ rows with $r + 1$ ones each. The average number of ones is

$$\frac{(n-1)r(r+1)}{(n-r)n^2}.$$

Corollary 4.9: *Let r be fixed, $p \equiv 1 \pmod{r}$ be prime and α be primitive in $\mathbb{F}_p$. The limit of the number of non-zero elements in $G(p, r, \alpha)$ as $p \to \infty$ is 0.*

This theorem and corollary are useful because they show that the $\mathbb{F}_2$-dual codes of $C(p, r, \alpha)$ also have the LDPC property.

5 Decoding Algorithm with Index Arrays

In this section we introduce a decoding algorithm for the codes obtained in Section 3. We study the MDS case, that is when $r = 2$. The code $\mathcal{C}_{\mathbb{F}_2^b}$ is an $\mathbb{F}_2$-linear code with length n, dimension $n-2$, minimum distance 3, with $b = n/2$, and corrects one error. However, one error in this case corresponds to b consecutive errors for the linear code $\mathcal{C}_{\mathbb{F}_2}$ over $\mathbb{F}_2$.

Let the index array A_H given in Table 2 represent the parity-check matrix of the code. Suppose we receive the word

$$\boldsymbol{x} = \begin{bmatrix} \xi_0 & x_{1,0} & x_{2,0} & \cdots & x_{b-1,0} \\ \xi_1 & x_{1,1} & x_{2,1} & \cdots & x_{b-1,1} \\ \vdots & \vdots & \vdots & & \vdots \\ \xi_{n-1} & x_{1,n-1} & x_{2,n-1} & \cdots & x_{b-1,n-1} \end{bmatrix}.$$

We superimpose the codeword on the index array, with each bit of the codeword corresponding with a cell of the array in Table 2:

0	ξ_0	1	ξ_1	$\cdots$	$n-1$	ξ_{n-1}
D_1	$x_{1,0}$	D_1+1	$x_{1,1}$	$\cdots$	D_1+n-1	$x_{1,n-1}$
D_2	$x_{2,0}$	D_2+1	$x_{2,1}$	$\cdots$	D_2+n-1	$x_{2,n-1}$
$\vdots$		$\vdots$			$\vdots$	
D_{b-1}	$x_{b-1,0}$	$D_{b-1}+1$	$x_{b-1,1}$	$\cdots$	$D_{b-1}+n-1$	$x_{b-1,n-1}$

We only consider the cells where the corresponding bit of the codeword is non-zero. Now, we construct the ith component of the vector of syndromes $s = (s_0, s_1, \ldots, s_{n-1})$ in the following way:

$$s_i = \left(\sum_{j=0}^{n-1} \sum_{k=1}^{b-1} x_{k,j} N_{k,j}^i + \xi_i \right) \bmod 2, \quad \text{for } i \in \mathbb{Z}_n, \tag{6}$$

where

$$N_{k,j}^i = \begin{cases} 1, & \text{if } i \in D_k + j, \\ 0, & \text{otherwise.} \end{cases}$$

Basically, s_i is the number of times that $i \in \mathbb{Z}_n$ appears in the index array.

If $s_{i_t} \neq 0$, for $t \in \{0, 1, \ldots, \ell\}$ with $\ell < n$ we know we have one error related to every index i_t, that is, the index i_t appears too many or not enough times in the index array. We locate these errors in one column of the array, since we can correct only one error in the word. As every column of the index array corresponds to a symbol of the codeword, we know which symbol of the codeword is in error. The position of the error in the symbol depends on the position of the cell with errors in the column. Let us see an example to illustrate this idea.

Example 7: Consider the index array given in Example 4:

0	1	2	3	4	5
$4,5$	$5,0$	$0,1$	$1,2$	$2,3$	$3,4$
$1,3$	$2,4$	$3,5$	$4,0$	$5,1$	$0,2$

This array represents the parity-check matrix of an $\mathbb{F}_2$-linear code of length 6, with dimension 4 and minimum distance 3 over $\mathbb{F}_2^3$.

If we receive the word

$$\boldsymbol{x} = [\ 010 \quad 101 \quad 011 \quad 010 \quad 001 \quad 001\ ]$$

and we know there is one error, we can correct it.

We write the word on the index array and we only consider the cells with a 1:

~~0~~ 0	1 1	~~2~~ 0	~~3~~ 0	~~4~~ 0	~~5~~ 0
4, 5 1	~~3~~, ~~0~~ 0	0, 1 1	1, 2 1	~~2~~, ~~3~~ 0	~~3~~, ~~4~~ 0
~~1~~, ~~3~~ 0	2, 4 1	3, 5 1	~~4~~, ~~0~~ 0	5, 1 1	0, 2 1

Now we count the number of times i appears in the array, for $i \in \mathbb{Z}_6$. If we compute these numbers modulo 2, we obtain the vector of syndromes. On the other hand, we can compute the components of the vector of syndromes $\boldsymbol{s}$ using expression (6). The components of the vector of syndromes are given by,

$$
\begin{aligned}
s_0 &= 2 \bmod 2 = 0, \\
s_1 &= 4 \bmod 2 = 0, \\
s_2 &= 3 \bmod 2 = 1, \\
s_3 &= 1 \bmod 2 = 1, \\
s_4 &= 2 \bmod 2 = 0, \\
s_5 &= 3 \bmod 2 = 1.
\end{aligned}
$$

The error is in one column where 2, 3 and 5 appear and the other indices are not affected. Then, the error should be in the column:

2
0, 1
3, 5

For example, the error could not be in the column

4
2, 3
5, 1

since the error in 5 would affect 1, and we obtain no errors in 1.

Then, the error is in the 2nd symbol of the word in the 0th and 2nd position. If we had 1 we change it by 0, and vice versa. Then, the corresponding corrected codeword is

$$\boldsymbol{x}^* = [\ 010 \quad 101 \quad 110 \quad 010 \quad 001 \quad 001\ ].$$

■

In this work we have studied the binary case, but it is possible to study the case where $q > 2$.

References

[1] M. Blaum, J. Brady, J. Bruck and J. Menon, EVENODD: An efficient scheme for tolerating double disk failures in RAID architectures, **42** (1995), 192–202.

[2] M. Blaum and J. Bruck, Decoding the Golay code with Venn diagrams, **36** (1990), 906–910.

[3] M. Blaum, J. Bruck and A. Vardy, MDS array codes with independent parity symbols, **42** (1996), 529–542.

[4] M. Blaum, P. G. Farrell and H. C. A. van Tilborg, Array codes, in *Handbook of Coding Theory* (eds. V. S. Pless and W. C. Huffman), Elsevier, North-Holland, 1998, 1855–1909.

[5] M. Blaum and R. M. Roth, New array codes for multiple phased burst correction, **39** (1993), 66–77.

[6] M. Blaum and R. M. Roth, On lowest density MDS codes, **45** (1999), 46–59.

[7] S. D. Cardell, *Constructions of MDS Codes over Extension Alphabets*, PhD thesis, Departamento de Ciencia de la Computación e Inteligencia Artificial, Universidad de Alicante, Alicante, España, 2012.

[8] S. D. Cardell, J.-J. Climent and V. Requena, A construction of MDS array codes, *WIT Transactions on Information and Communication Technologies*, **45** (2013), 47–58.

[9] S. D. Cardell and A. Fúster-Sabater, Recovering decimation-based cryptographic sequences by means of linear CAs, 2018, URL `https://arxiv.org/abs/1802.02206`. Retrieved 2018-November-30, from the arXiv database.

[10] G. A. Gibson, *Redundant Disk Arrays*, PhD thesis, Cambridge, MA: MIT Press.

[11] K. Huber, Some comments on Zech's logarithms, **36** (1990), 946–950.

[12] A. Kotzig, Hamilton graphs and Hamilton circuits, *Theory of Graphs and its Applications (Proc. Sympos. Smolenice, 1963)*, (1964), 63–82.

[13] E. Louidor and R. M. Roth, Lowest density MDS codes over extension alphabets, **52** (2006), 46–59.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 6th edition, North-Holland, Amsterdam, 1988.

[15] M. Sudan, *Algorithmic Introduction to Coding Theory*, 2002, URL `https://people.csail.mit.edu/madhu/FT02/scribe/lect16.ps` accessed 2018-November-30.

[16] L. Xu, V. Bohossian, J. Bruck and D. G. Wagner, Low-density MDS codes and factors of complete graphs, **45** (1999), 1817–1826.

[17] L. Xu and J. Bruck, X-code: MDS array codes with optimal encoding, **45** (1999), 272–276.

[18] G. V. Zaitzev, V. A. Zinov'ev and N. V. Semakov, Minimum-check-density codes for correcting bytes of errors, erasures, or defects, *Problems of Information Transmission*, **19** (1983), 197–204.